Zeszyty **PRASOZNAWCZE**

Kraków 2017, T. 60, nr 1 (229), s. 155–171

doi: 10.4467/22996362PZ.17.012.6778

www.ejournals.eu/Zeszyty-Prasoznawcze/

PRYWATNOŚĆ INFORMACYJNA W USŁUGACH AUDIOWIZUALNYCH Z PERSPEKTYWY NOWYCH ROZPORZĄDZEŃ UNIJNYCH (RODO I EPR)

BOGDAN FISCHER

Uniwersytet Jagielloński
Wydział Zarządzania i Komunikacji Społecznej

ABSTRACT

Information privacy in audiovisual services from the perspective of the new EU regulations (GDPR and EPR)

This article attempts to answer the question whether new and planned solutions for the protection of personal data and privacy are complementary to current media products and services. The analysis covers the approved scope of data protection in electronic communications and, in that context, information autonomy and information privacy. In the examined system of regulatory framework, i.a. electronic messages are protected, regardless of whether they relate to natural or legal persons, and any processing of electronic communications data will be subject to legal protection.

Keywords: media policy, audiovisual media services, information privacy, information autonomy, right to privacy, end device, end user, metadata

✉ Adres do korespondencji: Uniwersytet Jagielloński, Wydział Zarządzania i Komunikacji Społecznej, Instytut Dziennikarstwa, Mediów i Komunikacji Społecznej; ul. S. Łojasiewicza 4, 30-348 Kraków; bogdan.fischer@uj.edu.pl

Realizacja celów polityki medialnej: rozwoju nowoczesnych technologii informatycznych oraz wolności wypowiedzi i prawa do informacji (w tym swobodnego przepływu danych) wymaga równoczesnego gwarantowania przez władzę publiczną nie tylko coraz silniejszej ochrony danych osobowych i prawa do prywatności, ale również jej komplementarności z obecnymi produktami i usługami medialnymi o niewątpliwie złożonym charakterze. Komplementarności wykraczającej szeroko poza ochronę praw osoby fizycznej oraz zapewniających ochronę także tych danych, które danymi osobowymi nie są. Osiągnięciu tego celu mają służyć obecne zmiany zarówno w regulacjach unijnych dotyczących mediów audiowizualnych, jak i ochrony prywatności i danych osobowych. Czy tak jest w rzeczywistości, ma pokazać poniższa analiza. Będzie ona prowadzona przy założeniu, że pomimo rozróżnienia między uregulowaniami dotyczącymi transmisji sygnału nadawczego i uregulowaniami dotyczącymi treści, w obszarze prawa do prywatności i ochrony danych osobowych, występują pomiędzy nimi powiązania, które w nowych i projektowanych rozwiązaniach unijnych są widoczne, ale także dość skomplikowane.

Audiowizualne usługi medialne

Polityka medialna, kształtowana w głównej mierze przez władze publiczne, jest jednym z elementów polityki publicznej, która zawiera w sobie uregulowania zarówno prawne, jak i pozaprawne w zakresie funkcjonowania mediów. Polityka medialna obejmuje m.in. zasady i formy postępowania z mediami audiowizualnymi. Obecnie trwają prace nad aktualizacją unijnych przepisów w sektorze audiowizualnym. Podstawowym aktem prawnym na tym obszarze jest jak na razie Dyrektywa 2010/13/UE Parlamentu Europejskiego i Rady z dnia 10 marca 2010 roku (wersja ujednolicona) w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących świadczenia audiowizualnych usług medialnych (Dyrektywa o audiowizualnych usługach medialnych, Dz.Urz. UE L 95/1 z 15.4.2010, s. 1 i n., dalej: Dyrektywa medialna). W tym samym czasie w zakresie ochrony danych osobowych i prawa do prywatności zdecydowano się na odejście od regulowania tych spraw dyrektywą i wprowadzenie rozporządzeń obowiązujących wprost w państwach członkowskich[1]. 10 stycznia 2017 roku został opublikowany projekt rozporządzenia ogólnego w sprawie poszanowania życia prywatnego i ochrony danych osobowych

[1] Rozporządzenia unijne stosownie do art. 288 TFUE mają zasięg ogólny, wiążą w całości i są bezpośrednio stosowane we wszystkich państwach członkowskich, stąd też w ramach takiej regulacji (rozporządzeniami) mamy do czynienia z zakazem transpozycji rozumianej jako działalność legislacyjna państwa członkowskiego polegająca na powielaniu przepisów rozporządzenia w prawie krajowym, por. Jaroszyński 2011. Dyrektywa ma charakter skutkowy, pozwalając na dobór metod i środków poszczególnym państwom członkowskim. Z tego względu przyjęte przez te państwa drogi mogą być odmienne (tak jak np. przy regulacji ochrony danych osobowych), co skutkuje brakiem spójności.

w łączności elektronicznej (uchylającego Dyrektywę 2002/58/WE[2]) – Rozporządzenie w sprawie prywatności i łączności elektronicznej: dalej EPR[3]. Natomiast w dniu 27 kwietnia 2016 roku przyjęto Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Dz.Urz. UE L Nr 119 z 2016 r., s. 1 i n. – dalej RODO). Rozporządzenie wejdzie w życie w dniu 25 maja 2018 r. i z tym dniem zostanie uchylona obowiązująca Dyrektywa 95/46/WE, na podstawie której przyjęto polską ustawę o ochronie danych osobowych. Zgodnie z przyjętymi założeniami w tym samym dniu ma wejść w życie EPR.

Dotychczas w porządku krajowym każdego z państw Unii Europejskiej obowiązywały odrębne ustawy regulujące zasady ochrony i przetwarzania danych osobowych. Uchwalone rozporządzenie RODO ma to zmienić, stwarzając jeden spójny system, zapewniający równą ochronę danych osobowych, na terenie całej Unii Europejskiej. Powodem dokonania reformy prawa ochrony danych osobowych na poziomie unijnym oraz zastąpienia obowiązującej dotychczas dyrektywy rozporządzeniem jest postępująca integracja wewnątrz Unii, zwiększenie przepływów danych osobowych między poszczególnymi państwami, a także potrzeba dostosowania obowiązującego prawa do zmieniającej się rzeczywistości, w szczególności w kontekście rozwoju technicznego oraz informatyzacji i cyfryzacji życia. Pomimo tego, że przepisy rozporządzenia zastępują dyrektywę, część dotychczasowych regulacji Dyrektywy 95/46 WE została przeniesiona na grunt nowych przepisów.

Wartości leżące u podstaw regulacji w dziedzinie audiowizualnych usług medialnych w UE doprowadziły do ustanowienia grup przepisów, które wspierają wolność wypowiedzi, pluralizm mediów, różnorodność kulturową, ochronę konsumentów i ochronę danych osobowych[4]. W środowisku, w którym dochodzi do konwergencji, związek Dyrektywy medialnej z przepisami o ochronie danych jest bardzo ścisły. Przetwarzanie danych osobowych jest często warunkiem funkcjonowania nowych usług, nawet jeśli dana osoba może nie być do końca świadoma faktu gromadzenia i przetwarzania jej danych osobowych. Z chwilą gdy dane wytworzone w trakcie korzystania z audiowizualnych usług medialnych odnoszą się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, stają się danymi osobowymi i w związku z tym wchodzą w zakres regulacji przepisów o ochronie danych osobowych[5]. Jeśli dane osobowe są jednocześnie danymi łączności elektronicznej (o czym dalej), podlegać będą rozporządzeniu EPR, które stanowi *lex specialis* w stosunku do RODO. Ochronie EPR podlegają, także dane

[2] Dz.Urz. WE L 201 z 31.07.2002 r. s. 54 i n. – w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej.

[3] Dostępna pod adresem: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=42692.

[4] Zielona księga. Przygotowanie do nadejścia w pełni zintegrowanych mediów audiowizualnych: wzrost gospodarczy, twórczość i wartości (COM/2013/0231 final).

[5] Por. tamże.

łączności elektronicznej, które odnoszą się do podmiotów niebędących osobami fizycznymi[6]. Przy regulacjach ochronnych musi być uwzględniany fakt, że media audiowizualne, tak jak inne towary i usługi, są objęte zasadami przyjętymi w UE, mającymi zapewnić ich swobodny obieg na jednolitym rynku europejskim, niezależnie od sposobu, dostarczania tych usług (telewizja, Internet itd.).

Trzeba zwrócić uwagę, że granice tradycyjnego rozróżnienia w ramach polityki audiowizualnej na regulacje w obszarze techniki i w odniesieniu do zawartości komunikowania mają coraz bardziej ograniczone znaczenie, w tym z punktu widzenia ochrony danych osobowych i prawa do prywatności. Przy czym, jak zostało zaznaczone na wstępie analizy, prowadzone są z zastrzeżeniem, że istotą usług łączności elektronicznej jest przekazywanie sygnałów w sieciach łączności elektronicznej, natomiast istotą usług audiowizualnych – dostarczanie treści. Coraz częściej dostawca tradycyjnych usług audiowizualnych jest jednocześnie dostawcą i usług audiowizualnych, i sieci. Także wewnątrz usług audiowizualnych niezależnie od ich kwalifikacji jako linearne czy nielinearne trzeba uwzględniać coraz więcej cech wspólnych. Mamy do czynienia z obiegiem, w którym odbiorca treści w pośredni sposób daje dostawcy usług medialnych możliwość poznania rozległych informacji na swój temat, w tym np. preferencji konsumenckich, różnych zainteresowań. Te informacje z kolei mogą być wykorzystane nie tylko dla świadczenia mu usług medialnych, ale także w inny sposób, np. w działalności reklamowej dostawcy[7].

Definicja legalna pojęcia „audiowizualna usługa medialna" zawarta jest w art. 1 ust. 1 pkt a) Dyrektywy medialnej. Zgodnie z tym przepisem, oznacza usługę w rozumieniu art. 56 i 57 Traktatu o funkcjonowaniu Unii Europejskiej, za którą odpowiedzialność redakcyjną ponosi dostawca usług medialnych i której podstawowym celem jest dostarczanie ogółowi odbiorców – przez sieci łączności elektronicznej w rozumieniu art. 2 lit. a) Dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 roku w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej[8] – audycji w celach informacyjnych, rozrywkowych lub edukacyjnych. Taka audiowizualna usługa medialna jest przekazem telewizyjnym albo audiowizualną usługą medialną na żądanie w rozumieniu tego przepisu. Audiowizualną usługą medialną jest również „handlowy przekaz audiowizualny"[9]. Dyrektywa reguluje więc przekazy telewizyjne i usługi na żądanie oraz programy o formie *quasi*-telewizyjnej, za które odpowiedzialność

[6] EPR używa zbiorczego pojęcia „osób prawnych", na inne podmioty poza osobami fizycznymi. Należy więc przez to pojęcie rozumieć także te podmioty prawa, które w świetle krajowych przepisów nie są osobami prawnymi, lecz posiadają zdolność prawną – w polskim prawie takimi podmiotami są przede wszystkim spółki osobowe. Trzeba mieć na względzie, że prawodawstwo unijne i pojęcia w nim stosowane są rozumiane autonomicznie, w oderwaniu od rozumienia i wykładni poszczególnych pojęć na gruncie prawa krajowego.

[7] Na temat usług na żądanie por. Chałubińska-Jetkiewicz 2015, s. 86–99.

[8] Dz.U. L 108 z 24.04.2002, s. 33–50.

[9] Proponowane są zmiany w definicji „audiowizualnej usługi medialnej" o dające się wyodrębnić części usług, które jako całość nie spełniają przesłanek audiowizualnej usługi medialnej.

redakcyjną ponosi dostawca usług[10]. Jak na razie wyłączone z zakresu Dyrektywy medialnej są treści udostępniane na platformach internetowych upowszechniających materiały audiowizualne, które podlegają przepisom Dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 roku w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (Dyrektywa o handlu elektronicznym). Proponowane w tej dyrektywie zmiany mają rozszerzyć odpowiedzialność z niej wynikającą także na te podmioty. Nie jest jednak (jak na razie) projektowane pełne rozszerzenie, proponowane rozwiązanie wskazuje na zastosowanie zasady „regulacji stopniowalnej". Stosowano tę zasadę już wcześniej, np. przy nakładaniu zróżnicowanych obowiązków na tradycyjne i nowe media, zależnie od ich wpływu na kształtowanie opinii publicznej. Stąd też usługi na żądanie podlegają znacznie mniejszym wymogom niż np. tradycyjna telewizja i ukształtowane są jako minimum niezbędne do wypełnienia standardów obowiązujących w Unii Europejskiej[11]. Wydaje się więc, że również obecnie, wykorzystując ten sposób regulacji – planowane są wymogi skierowane do platform udostępniania plików wideo (*video-sharing platforms*). W szczególności mają być one spójne z Dyrektywą o handlu elektronicznym w takim znaczeniu, że platformy nie mogą być zobowiązane do generalnego monitorowania treści zamieszczanych przez użytkowników. Państwa UE nie będą mogły więc nakładać na takie platformy obowiązków w zakresie szerszym, niż określa to Dyrektywa o handlu elektronicznym. W ramach swojej odpowiedzialności dostawcy platform udostępniania plików wideo powinni stosować ochronę małoletnich oraz w zakresie przeciwdziałania mowie nienawiści. A jako preferowany sposób – współregulację.

Prawo do prywatności a prywatność informacyjna

Przedmiotem ochrony na tle współczesnych ujęć prawa do prywatności są wartości, które akcentują możliwość prowadzenia swoich spraw, decydowania o swoim życiu i o rodzajach więzi personalnych z innymi, z maksymalną swobodą, a zarazem z najmniejszym stopniem ingerencji świata zewnętrznego w tę sferę, która jest domeną własnej aktywności jednostki[12]. Prawo do prywatności od początku, gdy zostało po raz pierwszy sformułowane, wciąż ewoluuje. Jako kategoria normatywna zostało zdefiniowane przez Louisa Brandeisa i Samuela Warrena wraz z określeniem jego zakresu pod koniec XIX wieku, w związku z rozwojem środków masowego przekazu (Warren, Brandeis 1890). Przez lata ulegało dy-

Proponuje się również usunięcie z definicji „audycji" wymogu jej porównywalności z formą i treścią rozpowszechniania telewizyjnego, jak również dodanie do tej definicji krótkich filmów wideo.

[10] Audiowizualne usługi medialne na żądanie. Przewidywana praktyka regulacyjna KRRiT (23.03.2011) [http://www.krrit.gov.pl/Data/Files/_public/Portals/0/dyrektywa/110323_audiowizualne_uslugi_medialne_na_zadanie.pdf].

[11] Tamże.

[12] Wyrok TK z dnia 12 listopada 2002 r., sygn. akt SK. 40/01 (Dz.U. 2002 Nr 194, poz. 1641).

namicznym zmianom, wychodząc od podstawowej zasady *common law* zapewnienia ochrony osobie i jej własności. Wpływ na kształt prawa do prywatności miały zmiany w życiu społecznym wynikające z nowych zagrożeń dla jednostki, związane m.in. z rozwojem prasy czy możliwościami utrwalania obrazu i głosu. Siłę i ekspansywność prawa do prywatności należy również wiązać z faktem braku jednej, szeroko uznanej definicji i pozostawania prywatności „pojęciową chimerą" (Wacks 1980, s. VII). Niektórzy badacze wskazywali wręcz na istnienie pojęciowej próżni, która towarzyszy prywatności (Rubenfeld 1989, s. 739). Rozwój nowoczesnych technologii informatycznych wymaga, aby prawo do prywatności współistniało z prawem do gromadzenia i rozpowszechniania informacji oraz swobodnym przepływem informacji.

Prawo do prywatności na podstawie ujęcia tradycyjnego[13] oraz pod wpływem prac Rady Europy rozumiane jest obecnie najczęściej jako prawo do bycia pozostawionym w spokoju (ang. *right to be let alone*) (Krotoszynski 2016), a w szerszym ujęciu wraz z towarzyszącym mu prawem do własnej tożsamości i godności. Pierwszą próbę sformułowania prawa do prywatności w polskiej literaturze podjął Andrzej Kopff, określając je jako „prawo jednostki do życia własnym życiem układanym według własnej woli z ograniczeniem do minimum wszelkiej ingerencji zewnętrznej" (Kopff 1972, s. 6). Przez swoją uniwersalność, ujęcie to pozostaje wciąż aktualne.

Dla dalszych rozważań niezbędne jest wskazanie na rodzaj prywatności, który będzie miał podstawowe znaczenie z punktu widzenia prowadzenia niniejszej analizy. Pomimo wydawałoby się już ugruntowanego pojęcia prawa do prywatności wciąż utrzymują się trudności z jednoznacznym jego zdefiniowaniem[14], podobnie jak z wyróżnieniem wchodzących w jego zakres przedmiotowy rodzajów prywatności. Wykorzystując rozróżnienie Krzysztofa Motyki, można wskazać na:

1. prywatność fizyczną, która odnosi się do integralności fizycznej jednostek i dostępu do osoby; także może być określana jako prywatność materialna;
2. prywatność decyzyjną, która umożliwia podejmowanie decyzji osobistych bez ingerencji władzy czy osób trzecich;
3. prywatność komunikacyjną, związaną z wolnością wypowiedzi i stowarzyszania się;
4. prywatność terytorialną, chroniącą pewne miejsca, zwłaszcza będące własnością danej jednostki;
5. prywatność informacyjną, związaną z danymi osobowym i kontrolą informacji na swój temat[15].

Prywatność fizyczna może być również określana jako prywatność materialna. W kontekście prowadzonych rozważań kluczowy jest ostatni rodzaj prywatności,

[13] Po raz pierwszy użył tego zwrotu Brandeis w swoim zdaniu odrębnym w sprawie Omstead v. United States 277 U.S.438 (1928); zob. Warren, Brandeis 1890, s. 195.

[14] Na temat pojęcia prawa do prywatności wciąż trwają dyskusje; zob. np.: Jay, Hamilton 2003, s. 35 i n.; Jaffey 2004, s. 157 i n.; Doyle, Bagaric 2005, s. 3–36; Leenes, Koops, De Hert 2008.

[15] Por. Motyka 2010, s. 35. Autor przywołuje: Abeyratne 2002, s. 90 i n.; por. także Scoglio 1998, s. 45 i n. Ten ostatni autor uwzględnia m.in. prywatność kształtującą osobowość jednostki, związaną z jej wewnętrznym rozwojem.

tj. informacyjnej, którego rozumienie w niniejszym artykule jest zbliżone do ujęcia Alana Westina (1967, s. 7) i Charlesa Frieda (1969, s. 475, 477, 478), czyli zdolności obywateli do kontroli informacji ich dotyczących, w tym relacji z innymi ludźmi i tego, kiedy i w jakim zakresie informacja o nas zostanie przekazana innym. Każda zasada prawna, która określa wolność i która została powołana dla zapewnienia bezpieczeństwa jednostki, jest jednocześnie tą zasadą, która określa jej obowiązki, a więc każda wolność jest jednocześnie obowiązkiem[16]. Z jednej strony wolność wypowiedzi (Fischer 2015), która może być realizowana zarówno przez wykonywanie prawa do informowania innych, jak i bycia informowanym, z drugiej strony obowiązki w zakresie zachowania prawa do prywatności innych osób. Faktycznie żadna wolność nie może być nieograniczona, lecz funkcjonuje z uwzględnieniem prawa obowiązującego wszystkich ludzi – pomiędzy tym, co jest dozwolone, a co zakazane. Powszechnie przyjętą granicą wolności jednego człowieka jest wolność drugiego[17].

Przeważający jest pogląd, że z prawa do prywatności wywodzić należy ochronę danych osobowych. Patrząc z drugiej strony, to właśnie przy ochronie danych osobowych celem nadrzędnym jest ochrona prywatności. Zasadniczym wspólnym założeniem jest wyłączenie ingerencji zewnętrznej w prawa jednostki – przy czym zasięg i przedmiot obu praw nie są tożsame. W literaturze zwraca się uwagę, iż ustawodawca nie chroni całej sfery prywatności w równym stopniu. W sposób szczególny, ustawowo – prawem publicznym chronione są dane osobowe, natomiast inne aspekty prywatności zasadniczo pozostawione są ochronie cywilnoprawnej[18]. Współczesne rozumienie sfery życia prywatnego w odniesieniu do danych osobowych przyjmuje objęcie ochroną każdej informacji osobowej, bez względu na jej zawartość treściową (Jay, Hamilton 2003, s. 35 i n.; Jaffey 2004, s. 157 i n.; Leenes, Koops, De Hert 2008). Mogą to być zarówno informacje neutralne jak i sensytywne, w tym narażające osobę na uczucie wstydu czy skrępowania (Fischer 2013, s. 87).

Chcemy mieć prywatność informacyjną, to musimy mieć kontrolę, a jak chcemy mieć kontrolę, to musimy mieć autonomię informacyjną. Zgodnie z utrwalonym orzecznictwem ochrona życia prywatnego, gwarantowana konstytucyjnie w art. 47, obejmuje również autonomię informacyjną, określoną w art. 51 Konstytucji (por. np. wyrok z 19 lutego 2002 r., U 3/01, OTK ZU Nr 1/2002, poz. 3). Autonomia informacyjna oznacza prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących siebie, a także prawo do sprawowania kontroli

[16] Zgodnie z Heglowską teorią państwa: „To samo, co jest prawem, jest również obowiązkiem, i to samo, co jest obowiązkiem, jest również prawem". Hegel 1990, s. 496–497.

[17] Zob. omówienie obszernej literatury nt. „wolności" i „wolności słowa" w kontekście prawa prasowego w: Sobczak 2008, s. 25–31; zob. także Szpor 1997.

[18] Mednis 2006, s. 119 i n. oraz wskazana tam literatura. Na temat już ugruntowanego pojęcia prawa do prywatności wciąż trwają dyskusje, zob. np. Jay, Hamilton 2003, s. 35 i n.; Jaffey 2004, s. 157 i n.; Doyle, Bagaric 2005, s. 4 i n.

nad takimi informacjami, jeśli znajdują się w posiadaniu innych podmiotów[19]. W wyroku z 20 stycznia 2015 roku Trybunał Konstytucyjny zauważył, że:

> W sferze autonomii informacyjnej normy konstytucyjne gwarantują jednostce ochronę przed pozyskiwaniem, przetwarzaniem, przechowywaniem i ujawnieniem, w sposób naruszający reguły przydatności, niezbędności i proporcjonalności *sensu stricto* […] (sygn. akt. K 39/12; Dz.U. 2015 poz. 142).

Szczegółowy zakres uprawnień w ramach autonomii informacyjnej może zostać wskazany na podstawie wielu orzeczeń Trybunału Konstytucyjnego[20]. Zobowiązanie do ujawnienia informacji o sobie, które stanowi ograniczenie autonomii informacyjnej, może być dokonane tylko w ustawie, w granicach zgodnych z konstytucyjną zasadą proporcjonalności (wymaganiami określonymi w art. 31 ust. 3 konstytucji). Dokonanie ingerencji wymaga określenia granic i jej przesłanek (Fischer, Świerczyńska-Głownia 2006, s. 14; Fischer 2011).

W literaturze przedmiotu H. Wang, N. Lee i C. Wang wyodrębniają rodzaje naruszeń w odniesieniu do autonomii informacyjnej. Są to naruszenia polegające na niedozwolonym dostępie do danych oraz niedozwolonym zbieraniu danych, bez powiadomienia konsumenta (np. adresu e-mail; historii przeglądania). Następna wyróżniona przez autorów kategoria to niedozwolony monitoring aktywności konsumenta w sieci (bez powiadomienia i zgody). Z kolei w odniesieniu do prywatnych danych konsumenta dokonywana jest niedozwolona analiza – bez zawiadomienia. Może ona prowadzić do wniosków na temat wzorów zachowań i preferencji konsumenckich. Jeśli chodzi o kolejne naruszenia, odnoszą się do niedozwolonego transferu. Chodzi o przekazywanie prywatnych informacji konsumenta innemu przedsiębiorcy, także bez powiadomienia oraz jego zgody. Kolejne wskazywane przez autorów naruszenia obejmują niechciane oferowanie swoich usług oraz niedozwolone przechowywanie. To ostatnie polega na przechowywaniu prywatnych informacji konsumentów w sposób niespełniający odpowiednich standardów bezpieczeństwa, co umożliwia nieautoryzowany dostęp do tych informacji (Wang, Lee, Wang 1998).

Potrzeba przeglądu i dalszych przekształceń w uregulowaniach ochrony danych osobowych i prawa do prywatności wynika wprost z RODO. Rozporządzenie to nie tylko samo wprowadza znaczne zmiany w zakresie oraz sposobie ochrony danych osobowych, ale wskazuje w motywie 173 i artykule 98 konieczność kompleksowych zmian innych aktów prawnych Unii z tego obszaru, w tym Dy-

[19] Po raz pierwszy zasadę autonomii informacyjnej sformułował i rozwinął niemiecki Federalny Trybunał Konstytucyjny w orzeczeniu z dnia 15 grudnia 1983 r., 1BvR 209/83: „w warunkach nowoczesnego przetwarzania danych", Konstytucja Republiki Federalnej Niemiec chroni jednostkę przed „nieograniczonym gromadzeniem, używaniem i przekazywaniem jej danych osobowych". Konstytucja gwarantuje również „prawo jednostki do zasadniczo samodzielnego stanowienia o ujawnianiu i używaniu jej danych osobowych", za: Barta, Litwiński 2009, s. 34.

[20] Przykładowo wyrok TK z 12.01.2002 r. SK 40/02, OTK-A 2002, nr 6 poz. 81.

rektywy e-privacy[21]. To między innymi spowodowało, że Parlament Europejski oraz Komisja podjęły prace nad zmianą regulacji dotyczącej powyższego zakresu, dla osiągnięcia spójności z innymi wprowadzanymi zmianami w unijnym prawie. Rezultatem prac było opublikowanie wskazanego na wstępie projektu EPR, którego postanowienia mają chronić podstawowe prawa i wolności człowieka, a w szczególności prawo do prywatności w związku z przetwarzaniem danych. Zrezygnowano w EPR, podobnie jak w dyrektywie, ze szczegółowego określania rodzaju tych praw i wolności oraz ich treści. W tym zakresie konieczne jest sięgnięcie do źródeł prawa międzynarodowego i prawa UE, w których prawa te zostały potwierdzone, jak np. w Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności czy w Karcie Praw Podstawowych Unii Europejskiej[22]. W prawie unijnym przez długi czas nie definiowano prawa do informacji i ochrony danych osobowych. W rezultacie, podstawą działań organów Unii Europejskiej były standardy ochrony wynikające z orzecznictwa Europejskiego Trybunału Praw Człowieka oraz orzecznictwa Trybunału Sprawiedliwości[23]. Jeśli chodzi o Kartę Praw Podstawowych UE, określa ona katalog podstawowych praw i wolności obywatela Unii Europejskiej. Znalazły się wśród nich art. 7 i 8, które stanowią o poszanowaniu życia prywatnego i komunikowania się oraz o prawie każdej osoby do ochrony danych osobowych, które jej dotyczą[24]. Dane te muszą być przetwarzane rzetelnie, w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania. Przestrzeganie tych zasad podlega kontroli niezależnego organu. Andrzej Wróbel, oceniając KPP, wskazuje, że zmiany stanu prawnego w tej dziedzinie są „rewolucyjne nie tylko z perspektywy zapewnienia należytego standardu ochrony praw

[21] Dyrektywa 2002/58/WE zastąpiła Dyrektywę z 15 grudnia 1997 r. 97/66/WE w sprawie przetwarzania danych osobowych i ochrony prywatności w dziedzinie telekomunikacji; szerzej: Fischer 2006.

[22] Karta Praw Podstawowych UE została proklamowana najpierw 7 grudnia 2000 r. w Nicei (Dz.Urz. UE C Nr 364, s. 1), a następnie 12 grudnia 2007 r. w Strasburgu (Dz.Urz. C Nr 303, s. 1 oraz Dz.Urz. UE z 2010 r. C Nr 83, s. 389).

[23] Por. Jabłoński, Wygoda 2002, s. 101–102, tamże szerzej na temat historycznych unormowań międzynarodowych prawa do informacji.

[24] Jacek Sobczak wskazuje, że analiza odpowiednich przepisów KPP, TFUE, TWE oraz Dyrektywy 95/46 WE przemawia za uznaniem ochrony danych osobowych za prawo podstawowe w unijnym porządku prawnym. Jednocześnie zwraca uwagę, że dwa praktycznie identyczne przepisy – art. 16 ust. 1 TFUE oraz art. 8 KPP – znalazły się w dwóch aktach prawa pierwotnego UE, ale przyjmuje że art. 16 ust. 1 TFUE stanowi rozwinięcie i uzupełnienie art. 8 KPP. Artykuł 8 KPP „pozostaje w związku z art. 7 KPP, a ten z kolei z art. 8 Europejskiej konwencji. Artykuł 8 KPP koresponduje z treścią art. 16 ust. 1 TFUE, ten zaś współbrzmi z treścią wstępu i art. 8c, 12 i 17 Dyrektywy 95/46/WE. Jego źródła upatrywać należy także w art. 286 TWE, w którym rozszerzono zakres podmiotowy obowiązku ochrony danych osobowych na instytucje i organy Wspólnoty. Zarówno jednak art. 16 TFUE, jak i art. 286 TWE, a także art. 8 KPP nie definiują pojęcia «danych osobowych» które należy rozumieć zgodnie z definicją z Dyrektywy 95/46/WE", por. Sobczak 2012 – komentarz do art. 8, pkt 4 i wskazana tam literatura; Fischer 2013, s. 102.

podstawowych w Unii Europejskiej, ale także w kontekście rozwoju koncepcji „wielopoziomowego" konstytucjonalizmu europejskiego (Wróbel 2012, s. V).

Ochrona danych osobowych i prywatności w sektorze komunikacji elektronicznej (łączności elektronicznej) to ochrona w sektorach telekomunikacji, teleinformatyki i mediów elektronicznych. Ze względu na konwergencję, czyli łączenie się tych sektorów w jeden, regulacje prawne obejmują łącznie elektroniczne sieci komunikacyjne i usługi komunikacyjne oraz urządzenia towarzyszące. Projekt rozporządzenia EPR wskazuje, że podstawowym aktem prawnym w zakresie ochrony danych osobowych jest RODO, niemniej, aby zapewnić odpowiednią ochronę w związku ze specyfiką komunikacji elektronicznej, EPR wprowadza dodatkowe rozwiązania. Podstawowym założeniem przyjętej konstrukcji jest stworzenie kompletnej, spójnej regulacji, która będzie miała zastosowanie niezależnie od użytych technologii komunikowania się na odległość, tak aby ochrona była rzeczywista – także w przyszłości, gdy mogą powstać nowe sposoby komunikacji elektronicznej. Przyjęcie przepisów EPR, podobnie jak w przypadku RODO, powodować będzie obowiązywanie wprost, we wszystkich krajach Unii Europejskiej, bez konieczności, wprowadzania odrębnych przepisów przez poszczególne państwa. Kraje UE będą mogły wprowadzić do swoich porządków prawnych jedynie takie przepisy, które będą niezbędne do należytego egzekwowania rozporządzenia[25].

Istotnym aspektem EPR jest odnoszenie się nie tylko do komunikatów, które aktywnie i świadomie są przesyłane do innych użytkowników, ale również tych, które przesyłane są pomiędzy sobą przez podłączone do sieci przedmioty, jeżeli zawierają one dane osobowe – M2M (machine to machine) / IoT (Internet of Things). Zagadnienie to jest zresztą również regulowane w RODO, jak i w rozporządzeniu NIS[26].

Rozporządzenie EPR w dużej mierze wprowadza zmiany i rozszerza dotychczasowe pojęcia zdefiniowane na gruncie dyrektywy, a także odsyła do definicji z innych unijnych aktów prawnych. W zakresie, w jakim EPR odnosi się do zagadnień ochrony danych osobowych, zastosowanie będą miały pojęcia RODO, w tym definicja przetwarzania, natomiast w zakresie zasad ochrony prywatności i zasad świadczenia usług łączności elektronicznej – pojęcia zawarte w dyrektywie Europejski Kodeks Komunikacji Elektronicznej (EECC), obecnie także w fazie projektowania. Znajdziemy tam wiele niezbędnych definicji, jak np. „usługa łączności elektronicznej" (usługa świadczona za pośrednictwem sieci łączności elektronicznej polegająca na dostępie do Internetu, czy też świadczenie usług łączności maszyna–maszyna, tzw. Internet rzeczy), czy „użytkownik końcowy",

[25] Będzie to skutkować koniecznością znaczącej zmiany ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tj. Dz.U. z 2016 r., poz. 1030, 1579), aby usunąć z niej przepisy, które byłyby sprzeczne z EPR lub stanowiłyby powtórzenie jego postanowień.

[26] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE z 19.7.2016, L 194, s. 1).

rozumiany jako podmiot, który korzystając z publicznie dostępnych usług łączności elektronicznej, nie udostępnia publicznych sieci lub usług (jest wyłącznie odbiorcą usługi i uczestnikiem sieci) itd.[27].

Wydaje się że jednym z ważniejszych wyzwań jest dokładne określenie wzajemnych relacji z RODO oraz wyeliminowanie odmiennych sposobów regulacji, zwłaszcza w obszarze dyrektyw konsumenckich[28]. W opinii unijnego ustawodawcy, wobec znacznego poszerzenia ochrony prywatności użytkowników sieci, przede wszystkim Internetu, niezbędne było szczegółowe określenie, czym jest komunikacja elektroniczna i co stanowi jej części składowe. Z tego też względu EPR wprowadza pojęcie połączenia elektronicznego, które będzie rozumiane, jako wymiana elektronicznych komunikatów pomiędzy skończoną liczbą użytkowników. W zakresie danych pochodzących z łączności elektronicznej EPR w art. 4 definiuje m.in. treść połączeń elektronicznych, które oznaczają tekst, głos, dźwięk, obraz. Z kolei metadane połączeń elektronicznych są definiowane jako wszelkie dane dotyczące użytkownika końcowego, przetwarzane na potrzeby transmisji, dystrybucji lub wymiany zawartości elektronicznego komunikatu. Będą nimi m.in. data, miejsce, długość trwania komunikatu, jego typ oraz przeznaczenie, jak również dane dotyczące urządzenia, umożliwiające zidentyfikowanie użytkownika końcowego.

Zakres stosowania EPR

Jeśli chodzi o zakres, EPR obejmuje przetwarzanie danych połączeń elektronicznych w związku z korzystaniem z usług łączności elektronicznej oraz przetwarzanie informacji związanych z urządzeniami końcowymi użytkowników końcowych realizowane przez szerokie spectrum podmiotów. Są nimi wszelkie podmioty zapewniające usługi łączności elektronicznej oraz prowadzące publicznie dostępne spisy abonentów, jak również podmioty, których działalność nie była dotychczas objęta regulacją e-privacy, zapewniające dostęp do oprogramowania umożliwiającego elektroniczną komunikację, tzw. OTT, czyli usługi Over-the-

[27] Wniosek z dnia 2.10.2016 r. Dyrektywa parlamentu Europejskiego i Rady ustanawiająca Europejski kodeks łączności elektronicznej (Wersja przekształcona) COM(2016) 590 final; por. Fischer, Mazewski 2017.

[28] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (Dyrektywa o handlu elektronicznym); Dyrektywa 2002/65/WE Parlamentu Europejskiego i Rady z dnia 23 września 2002 r. dotycząca sprzedaży konsumentom usług finansowych na odległość oraz zmieniająca Dyrektywę Rady 90/619/EWG oraz Dyrektywy 97/7/WE i 98/27/WE; Dyrektywa 2005/29/WE Parlamentu Europejskiego i Rady z dnia 11 maja 2005 r. dotycząca nieuczciwych praktyk handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym oraz zmieniająca Dyrektywę Rady 84/450/EWG, Dyrektywy 97/7/WE, 98/27/WE i 2002/65/WE Parlamentu Europejskiego i Rady; Rozporządzenie (WE) nr 2006/2004 Parlamentu Europejskiego i Rady (Dyrektywa o nieuczciwych praktykach handlowych).

-Top communication services, np. komunikatory. Ponadto EPR ma także zastosowanie do jakichkolwiek podmiotów, które korzystając z usług łączności elektronicznej, zbierają informacje o użytkownikach końcowych lub kierują do nich reklamy, wykorzystując środki marketingu bezpośredniego – a zatem podmiotów, które poprzez swoje usługi monitorowania umożliwiają reklamodawcom profilowanie reklam dla konkretnego użytkownika. Nie chodzi jednak o wyłączenie możliwości profilowania, ale o to, by każdy użytkownik miał prawo sam zdecydować, czy chce, by ktokolwiek śledził jego zachowanie w sieci w celach reklamowych, a jeśli tak, to w jakim zakresie i w jakim celu (Fischer, Mazewski 2017).

Proponowany zakres ochrony EPR jest bardzo szeroki i ma obejmować dużo większą liczbę podmiotów, niż ma to miejsce obecnie. Obowiązanymi będą wszystkie podmioty prowadzące strony internetowe umożliwiające wzajemną komunikację użytkowników, podmioty dostarczające oprogramowania w postaci przeglądarek internetowych czy różnego typu aplikacji instalowanych na komputerach, smartfonach, tabletach itp., które będą przetwarzać jakiekolwiek dane osobowe w rozumieniu RODO lub dane połączeń elektronicznych. Właściwie każdy podmiot, który w jakikolwiek sposób wykorzystuje nowoczesne technologie komunikacji z klientami, będzie zobowiązany do wdrożenia i przestrzegania regulacji zawartych w EPR, nawet jeśli działalność usług łączności elektronicznej nie jest jego podstawową działalnością, a np. tworzy aplikację na smartfon umożliwiającą dostęp do konta.

Ważnym założeniem przyjmowanym zarówno w RODO, jak i EPR jest jak najszersza ochrona podmiotów z UE oraz na terytorium UE. Każda usługa, która ostatecznie jest wykonywana na terenie UE lub użytkownik końcowy zamieszkały w Unii z niej korzysta, będzie musiała spełniać wszelkie wymogi przewidziane w EPR. Stąd też, niezależnie od tego, czy usługa łączności elektronicznej jest płatna czy darmowa, EPR będzie miało zastosowanie do wszystkich takich usług na rzecz użytkowników końcowych zamieszkujących w UE. Ochrona EPR obejmuje także informacje związane z urządzeniem końcowym należącym do użytkownika końcowego, zamieszkującego w UE. Rozszerzony w stosunku do Dyrektywy e-privacy zakres zastosowania EPR obejmuje poza tradycyjnymi środkami łączności elektronicznej (np. telefon, SMS) wspomniane wyżej usługi OTT, a także komunikację M2M, o ile przetwarzają dane osobowe lub informacje dotyczące użytkowników końcowych[29].

Wyłączone spod obowiązywania EPR są działania leżące poza kompetencją Unii, usługi łączności elektronicznej niedostępne publicznie (np. wewnętrzne systemy w przedsiębiorstwach), a także przetwarzanie takich komunikatów przez organy państw członkowskich UE, spowodowane koniecznością zapewnienia bezpieczeństwa wewnętrznego kraju, obrony czy też egzekwowania krajowego prawa karnego. Brak przepisów w tym zakresie powoduje, że ewentualne prze-

[29] Do przestrzegania przepisów EPR będą zobowiązane także podmioty, które udostępniają hotspoty, czyli publicznie dostępne sieci Wi-Fi; por. Fischer, Mazewski 2017.

twarzanie przez władze państwowe poufnych komunikatów może się stać zasadą, a nie wyjątkiem – jak zakłada EPR.

Zgodne z prawem przetwarzanie danych łączności elektronicznej

Podstawę świadczenia jakiejkolwiek usługi łączności elektronicznej, podobnie jak na gruncie dotychczasowej Dyrektywy e-privacy, stanowi zasada poufności określona w art. 5 EPR, zgodnie z którą jakiekolwiek ingerencje w połączenie elektroniczne, takie jak podsłuchiwanie, monitorowanie, skanowanie, nagrywanie czy przetwarzanie, przez jakikolwiek podmiot bez zgody użytkowników końcowych jest zakazane, o ile EPR nie stanowi inaczej. Możliwość przetwarzania takich danych jest zatem wyłączona, poza ściśle określonymi w EPR wyjątkami. Po nawiązaniu komunikacji pomiędzy użytkownikami przetworzona treść musi zostać niezwłocznie usunięta lub zanonimizowana. Przy czym dozwolone będzie zapisywanie lub przechowywanie tych danych przez użytkowników końcowych lub podmiot trzeci, o ile podmiot ten będzie spełniał wymogi przetwarzania określone w RODO (np. zgoda, umowa, przepisy prawne). Z kolei metadane muszą zostać usunięte lub zanonimizowane, gdy nie będą już potrzebne do osiągnięcia celu w postaci przeprowadzenia transmisji lub połączenia. W przypadku ich przetwarzania do rozliczania usług (wynagrodzenia) mogą być przechowywane do czasu, gdy zapłata może być skutecznie dochodzona w świetle krajowego prawa, czyli w praktyce do czasu przedawnienia roszczenia o zapłatę (Fischer, Mazewski 2017).

Zgoda i jej znaczenie

Na każde przetwarzanie treści i metadanych, które są niezbędne do zrealizowania usługi, a zatem przede wszystkim wszelkiego rodzaju działania marketingowe czy reklamowe, wymagana jest zgoda. Zasadą powszechnie przyjmowaną zarówno w doktrynie, jak i orzecznictwie jest przyznanie podstawowego znaczenia (z zastrzeżeniem określonych wyjątków)[30] przesłance zgody osoby zainteresowanej na udostępnianie informacji[31].

Wzrost znaczenia zgody w stosunku do poprzedniej regulacji zawartej w dyrektywie jest istotny. Zgoda uzyskiwana przez dostawcę usług na gruncie EPR będzie musiała spełniać wymogi i rygory RODO, a więc być świadomą, konkretną, jednoznaczną i dobrowolną. Podejście do tej kwestii w różnych aktach prawnych nie jest jednolite, co może powodować problemy w stosowaniu ich postanowień. Przykładowo, Dyrektywa o handlu elektronicznym, której przepisy transpono-

[30] W szczególności w określonych przypadkach ograniczających swobodne wyrażenie woli w stosunkach pracowniczych.

[31] Zob. wyrok TK z 12.01.2002 r. SK 40/02, OTK-A 2002, nr 6 poz. 81; zob. Safjan 2002, s. 238.

wano do polskiego ustawodawstwa m.in. w ustawie o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2004 roku[32], nie zawiera w swoich postanowieniach regulacji, które wprost odsyłałyby do definicji zgody zawartej w innych aktach prawnych, jak również nie nakazuje, aby spełniała ona określone w innych przepisach wymogi. Taka sytuacja może doprowadzić do tego, że w zakresie uzyskiwanych przez dostawców zgód będą stosowane różne reżimy prawne.

Ochrona informacji związanych z urządzeniami końcowymi użytkowników końcowych

Projektowaną nowością na gruncie EPR jest ochrona informacji znajdujących się na urządzeniach końcowych oraz danych związanych z tymi urządzeniami, takich jak ich parametry, funkcje, oprogramowanie, aktywność użytkownika w sieci itp. EPR odsyła do definicji zawartej poza tym rozporządzeniem, a mianowicie do Dyrektywy Komisji 2008/63/WE z dnia 20 czerwca 2008 roku w sprawie konkurencji na rynkach końcowych urządzeń telekomunikacyjnych, przez które należy rozumieć każde urządzenie podłączone do sieci publicznej w celu przesyłania, przetwarzania lub odbierania informacji – a zatem przede wszystkim komputery, smartfony czy tablety. Urządzenia końcowe to sfera naszej prywatności i jako taka powinna podlegać ochronie przed niechcianym przez nas śledzeniem, bez względu na zastosowaną technologię, np. skrypty śledzące, wtyczki, ukryte identyfikatory, ciasteczka (cookies). Dotychczasowa Dyrektywa o e-privacy również przewidywała ochronę przed śledzeniem, ale ograniczała ją zasadniczo do użycia cookies.

Zbieranie danych urządzeń końcowych lub z nimi związanych będzie zakazane z wyłączeniem przypadków, gdy: jest to niezbędne wyłącznie w celu zrealizowania transmisji w danej komunikacji; użytkownik końcowy wyraził na to uprzednią zgodę; jest to niezbędne dla zapewnienia usług społeczeństwa informacyjnego, których zażądał użytkownik (czyli wszelkiego rodzaju portale społecznościowe).

Zbieranie danych wysyłanych przez samo urządzenie końcowe w celu umożliwienia połączenia się z innym urządzeniem lub siecią będzie zakazane, chyba że jest realizowane wyłącznie w celu zapewnienia połączenia. W jasny i widoczny sposób musi zostać podana do publicznej wiadomości informacja, z której będzie wynikać co najmniej sposób zbierania danych, cel zbierania danych, dane podmiotu odpowiedzialnego. Ponadto informacje, jakie zgodnie z RODO musi podać administrator oraz dotyczące tego, co użytkownik końcowy może przedsięwziąć, aby wyłączyć lub zminimalizować zbieranie takich danych. Oznacza to, że w praktyce podmiot, który chce uzyskiwać dane, np. dotyczące lokalizacji urządzenia, będzie musiał spełniać warunki informacyjne podczas uruchamiania aplikacji lub otwarcia strony internetowej obejmujące sposób i cel zbierania ta-

[32] Tj. z dnia 15 lipca 2016 r. (Dz.U. 2016, poz. 1030).

kich danych, a także sposób umożliwiający użytkownikowi wyłączenie takiego dostępu do danych.

Podsumowanie

Przez nowe rozwiązania zawarte w RODO i EPR przechodzimy na wyższy poziom ochrony danych osobowych i prywatności oraz jej komplementarności. Każdy komunikat przesyłany drogą elektroniczną, który może zawierać dane osobowe, jest traktowany jako poufny i odpowiednio chroniony przed bezprawnym przechwyceniem. Przy przejęciu komunikatu i danych transmisyjnych z nim zawiązanych brana jest pod uwagę okoliczność, że obecnie może tego dokonać nie tylko człowiek, ale także maszyna. Stosowana jest więc ochrona nie tylko tam, gdzie człowiek zbiera informacje o człowieku, ale także gdy przedmioty i urządzenia zbierają informacje o ludziach. Ochrona taka staje się eksterytorialna. Chroniony jest coraz szerszy zakres danych, nie tylko indywidualne komunikaty i dane transmisyjne, ale także wszelkie inne. Duży nacisk kładziony jest na ochronę metadanych, z istnienia których wiele osób nie zdaje sobie sprawy. Dotyczy ona wszelkich elementów łączności elektronicznej, a nie jedynie danych osobowych przekazywanych w związku z jej prowadzeniem. Z prywatności informacyjnej wykształciła się ochrona danych osobowych. Z kolei podstawę ochrony tych danych stanowi autonomia informacyjna, chociaż nie ma charakteru bezwzględnego – podlega wyłącznie ograniczeniom legalizowanym przez ustawodawcę (także unijnego) i to z wyłączeniem arbitralności jego działań. Nie mogą więc występować inne (pozaustawowe) ograniczenia. Rozwój nowoczesnych technologii informatycznych, jak i niewłaściwie rozumiane prawo do informacji nie mogą wyłączać autonomii informacyjnej i decydowania o tym, co na nasz temat udostępnimy lub co na nasz temat się zbiera. Elektroniczne komunikaty są objęte ochroną niezależnie od tego, czy dotyczą one osób fizycznych czy prawnych (w szerszym rozumieniu unijnym) – w przeciwieństwie do zasad ochrony danych osobowych. Z tego też względu każde przetwarzanie danych łączności elektronicznej będzie podlegało ochronie prawnej, mimo że w odniesieniu do poszczególnych podmiotów mogą być chronione odmienne dobra, jak np. u osób prawnych – tajemnica przedsiębiorstwa. Utrzymano jednocześnie komplementarność pomiędzy polityką dotyczącą usług łączności elektronicznej i audiowizualnych usług medialnych. Wydaje się, że na tym etapie można określić omawiane rozwiązania jako spójny system ram regulacyjnych, umożliwiający z jednej strony rozwój audiowizualnych usług medialnych, z drugiej w założeniach odpowiadający na potrzeby w zakresie poufności, ochrony danych osobowych, prawa do prywatności. Nie jest to jednocześnie system, który by nie miał wad i niespójności. Niektóre z nich są widoczne już teraz, co może wywołać zmiany – zwłaszcza ze względu na etap projektowania, w którym znajduje się większość analizowanych rozwiązań. Wiele problemów ukaże zapewne dopiero praktyka stosowania.

Bibliografia

Abeyratne R. (2002). Attacks on America – Privacy Implications of Heightened Security Measures in the United States, Europe, and Canada. *Journal of Air Law and Commerce*, vol. 67, s. 83–115.

Barta P., Litwiński P. (2009). Ustawa o ochronie danych osobowych. Komentarz. Warszawa.

Chałubińska-Jetkiewicz K. (2015). Ochrona prywatności w audiowizualnych usługach medialnych na żądanie. *Internetowy Kwartalnik Antymonopolowy i Regulacyjny*, nr 7 (4), s. 86–99.

Doyle C., Bagaric M. (2005). The Right to Privacy: Appealing but Flowed. *International Journal of Human Rights*, vol. 9, no. 1, s. 3–36.

Fischer B. (2006). Tajemnica telekomunikacyjna w świetle dyrektyw UE i w prawie polskim. *Europejski Przegląd Sądowy*, nr 11, s. 29–35.

Fischer B. (2011). Prawo użytkowników wyszukiwarek internetowych do poszanowania ich autonomii informacyjnej. W: G. Szpor (red.). Internet. Ochrona wolności, własności i bezpieczeństwa (s. 63–72). Warszawa.

Fischer B. (2013). *Cloud computing* – globalny technologiczny paradygmat – zagrożeniem dla ochrony danych osobowych i prywatności. Kraków.

Fischer B. (2015). Wolność wypowiedzi prasowej a prawo do bycia zapomnianym. W: J. Gołaczyński (red.). Jawność i jej ograniczenia. Tom VIII: Postępowania sądowe (s. 91–109). Warszawa.

Fischer B., Mazewski M. (2017). Projektowane rozporządzenie e-privacy, lex specialis RODO [http://mojafirma.infor.pl/e-firma/technologia/753009,Projektowane-rozporzadzenie-eprivacy-lex-specialis-RODO.html].

Fischer B., Świerczyńska-Głownia W. (2006). Dostęp do informacji ustawowo chronionych, zarządzanie informacją. Kraków.

Fried C. (1969). Privacy: A Moral Analysis. *Yale Law Review*, vol. 77, no. 1, s. 475–949.

Hegel G.W.F. (1990). Encyklopedia nauk filozoficznych. Warszawa.

Jabłoński M., Wygoda K. (2002). Dostęp do informacji i jego granice. Wrocław.

Jaffey P. (2004). Rights of Privacy. Confidentiality, and Publicity, and Related Rights. W: P.L.C. Torremans (ed.). Copyright and Human Rights. Freedom of Expression-Intellectual Property-Privacy (s. 447–473). The Hague–London–New York.

Jaroszyński T. (2011). *Rozporządzenie* Unii Europejskiej jako składnik systemu prawa obowiązującego w Polsce. Warszawa.

Jay R., Hamilton A. (2003). Data Protection, Law and Practice. London.

Kopff A. (1972). Koncepcja praw do intymności i do prywatności życia osobistego. *Studia Cywilistyczne*, t. 20, s. 3–44.

Krotoszynski R.J. (2016). Privacy Revisited: A Global Perspective on the Right to Be Left Alone. Oxford University Press.

Leenes R.E., Koops B., De Hert P. (2008). Constitutional Rights and New Technologies: A Comparative Study. Haga.

Mednis A. (2006). Prawo do prywatności a interes publiczny. Warszawa.

Motyka K. (2010). Prawo do prywatności. *Zeszyty Naukowe Akademii Podlaskiej w Siedlcach*. Seria: *Administracja i Zarządzanie*, t. 85, s. 9–36.

Rubenfeld J. (1989). The Right of Privacy. *Harvard Law Review*, vol. 102, s. 737–807.

Safjan M. (2002). Refleksje wokół konstytucyjnych uwarunkowań rozwoju ochrony dóbr osobistych. *Kwartalnik Prawa Prywatnego*, z. 1, s. 223–246.

Scoglio S. (1998). Transforming Privacy: A Transpersonal Philosophy of Rights. Westport, CT.

Sobczak J. (2012). Komentarz do artykułu 8, pkt 4. W: A. Wróbel (red.). Karta Praw Podstawowych Unii Europejskiej. Komentarz. Warszawa.
Sobczak J. (2008). Prawo prasowe. Komentarz. Warszawa.
Szpor G. (red.) (1997). Wolność informacji i jej granice. Katowice.
Wacks R. (1980). The Protection of Privacy. London.
Wang H., Lee M.K., Wang C. (1998). Consumer privacy concerns about Internet marketing. *Communications of the ACM*, vol. 41 (3), s. 63–70.
Warren S.D., Brandeis L.D. (1890). The Right to Privacy. *Harvard Law Review*, nr 4, s. 193–220.
Westin A.F. (1967). Privacy and Freedom. London.
Wróbel A. (2012). Przedmowa. W: A. Wróbel (red.). Karta Praw Podstawowych Unii Europejskiej. Komentarz (s. V). Warszawa.

STRESZCZENIE

Artykuł stanowi próbę odpowiedzi na pytanie, czy nowe i planowane rozwiązania w zakresie ochrony danych osobowych i prywatności są komplementarne z obecnymi produktami i usługami medialnymi. Analizie został poddany zakładany zakres ochrony danych w komunikacji elektronicznej i na tym tle autonomia informacyjna i prywatność informacyjna. W badanym systemie ram regulacyjnych są objęte ochroną m.in. elektroniczne komunikaty niezależnie od tego, czy dotyczą one osób fizycznych czy prawnych; każde przetwarzanie danych w łączności elektronicznej będzie podlegało ochronie prawnej.

Słowa kluczowe: polityka medialna, audiowizualne usługi medialne, prywatność informacyjna, autonomia informacyjna, prawo do prywatności, urządzenie końcowe, użytkownik końcowy, metadane